

Demystifying Third-Party Risk Management

Protecting Your Organization in an Interconnected World

A STRATEGIC IMPERATIVE FOR MODERN BUSINESS

Key Partnerships

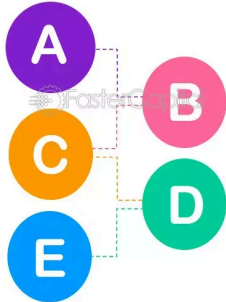
Collaborative Ventures



Distribution Networks



Research and Development Collaborations



Supplier Relationships



Co-Marketing Initiatives



Why Third-Party Risk Matters Now More Than Ever

- Modern businesses operate through **complex networks of vendors and partners**
- Organizations no longer operate in isolation—success depends on **third-party relationships**
- Third-party failures directly impact your **brand, reputation, and bottom line**
- The stakes are higher than ever: data breaches, service outages, and **regulatory penalties**

Third-Party Breaches: When Partners Become Your Vulnerability

3.3 Million People Exposed

Background check firm breach compromised names, Social Security numbers, and driver's license numbers

Healthcare Data Compromised

Third-party provider failure led to exposure of sensitive patient medical information and Social Security numbers


GrubHub Customer Data Exposed

Third-party support provider breach exposed customer and driver information, including payment details

2,300+ Retirement Plan Participants Affected


Insider threat at third-party call center resulted in improper access of Social Security and account numbers

How to prevent data breaches




1

Teach your team regularly




6

Strengthen network security




2

Make strong passwords a must




7

Aim for zero-trust security




3

Add multi-factor authentication




8

Prepare a response plan




4

Keep everything up to date



9

Back up your data



5

Add Identity and Access Management tools

*

*

*

*

*

The Cascading Consequences of Third-Party Failures

Operational Disruption

Payment processor downtime halts sales transactions and directly impacts revenue and customer experience

Single point of failure = core business impact

Regulatory Penalties

DORA, GDPR, HIPAA, CCPA, OCC guidance mandate effective TPRM programs

Non-compliance = significant fines and penalties

Brand Damage

Public sees your company name in headlines, not the vendor's name

Reputation erosion = long-term market impact

Customer Churn

Loss of trust is the most damaging and long-lasting consequence

Eroded confidence = reduced customer lifetime value

Building a Fortress: The Five-Step TPRM Framework (Part 1)

1 Planning & Due Diligence

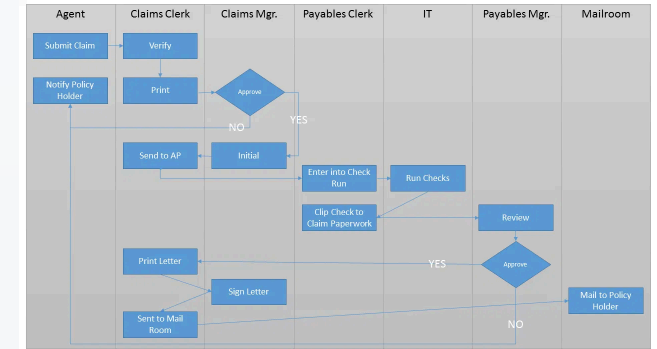
Conduct **objective, in-depth assessment** of vendor capabilities, security practices, and financial stability to ensure they are a secure and stable partner

2 Contracting

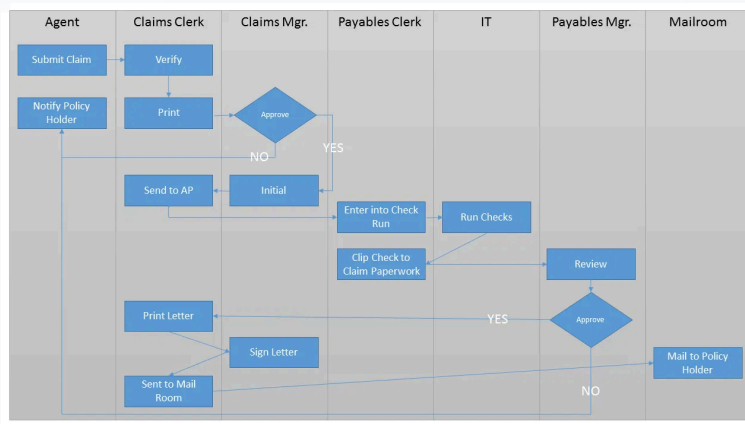
Establish formal, written agreements with **specific security and compliance requirements**, including data breach notifications, audit rights, and data protection controls

3 Risk Assessment

Conduct deep, formal evaluation of vendor's **IT security controls and data privacy practices** using detailed questionnaires to ensure compliance with organizational standards



Vigilance Never Stops: Continuous Monitoring & Remediation



4 Continuous Monitoring

Risk-based monitoring to catch emerging threats in real-time. Many organizations only assess vendors **1-2 times yearly**, leaving vulnerabilities unchecked for extended periods.

Real-time risk intelligence enables proactive threat detection

5 Remediation & Offboarding

Fix identified risks through vendor collaboration, then securely end relationships by revoking all access to sensitive data and systems. Ensures data security **after partnership ends**.

Complete lifecycle management protects your organization at every stage



What Your Board Needs to Know

1

TPRM is not a **technical chore**—it's a **strategic business imperative**

2

Regulatory bodies worldwide now mandate TPRM programs (DORA, GDPR, HIPAA, CCPA, OCC)

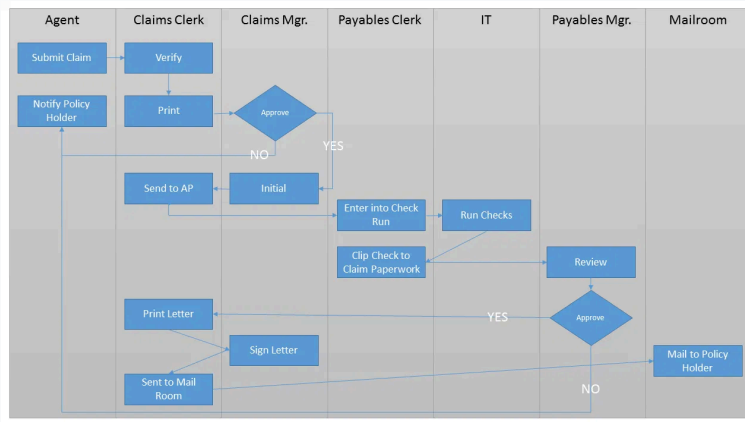
3

Failure to implement TPRM = **regulatory fines, brand damage, and operational risk**

4

Your organization remains **responsible for third-party actions**, regardless of outsourcing

Implementing TPRM: From Strategy to Action



- 1 Establish a **formal TPRM governance structure** with clear accountability and executive sponsorship
- 2 Develop **risk-based vendor assessment criteria** aligned with business criticality and regulatory requirements
- 3 Implement **continuous monitoring systems** to detect emerging threats in real-time
- 4 Include **third-party outage scenarios** in incident response and business continuity plans
- 5 Regularly **review and update TPRM policies** to address evolving threats and regulations

Your Shield in an Interconnected World

Success in today's **globalized economy** depends on managing **third-party relationships strategically**. No business operates in a vacuum.

TPRM is not a **compliance checkbox**—it's **essential for protecting** your organization's most valuable assets

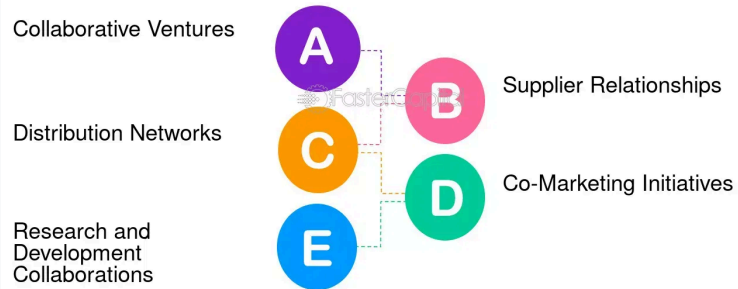
By systematically vetting partners, setting clear rules, and maintaining **vigilant oversight**, TPRM acts as your shield

Protect your **data**, ensure **operational stability**, and maintain **customer trust**

TPRM is a core strategic imperative for survival and success in an interconnected world.



Key Partnerships



Questions & Next Steps

Ready to strengthen your **TPRM program** and protect your organization in an interconnected world?

- **Assess your current state:** Evaluate existing vendor management practices against the TPRM framework
- **Identify gaps:** Determine which TPRM components need strengthening or implementation
- **Develop roadmap:** Create a prioritized implementation plan aligned with business objectives
- **Secure governance:** Establish executive sponsorship and cross-functional accountability

Let's discuss how to build your organizational shield.

Contact us to schedule a follow-up discussion and explore tailored TPRM solutions for your organization.